REMARKS

The Office Action dated January 29, 2009, has been received and carefully considered. In this response, claims 1, 12, 21, and 23 have been amended, and claims 2 and 13 have been cancelled without prejudice. No new matter has been added. Entry of the amendments to claims 1, 12, 21, and 23, and the cancellation of claims 2 and 13 without prejudice is respectfully requested. Reconsideration of the current rejections in the present application is also respectfully requested based on the following remarks.[1]

I. THE OBVIOUSNESS REJECTION OF CLAIMS 1-6, 9, 12-17, & 20-24

On page 2 of the Office Action, claims 1, 3-6, 9, 12, 14-17, and 20-22 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Peng et al. ("Peng") ("Detecting Distributed Denial of Service Attacks Using Source IP Address Monitoring") in view of U.S. Patent No. 5,828,846 to Kirby et al. ("Kirby"). This rejection is hereby respectfully traversed.

[1] As Applicant's remarks with respect to the Examiner's rejections are sufficient to overcome these rejections, Applicant's silence as to assertions made by the Examiner in the Office Action or certain requirements that may be applicable to such rejections (e.g., assertions regarding dependent claims, whether a reference constitutes prior art, whether references are legally combinable for obviousness purposes) is not a concession by Applicant that such assertions are accurate or such requirements have been met, and Applicant reserves the right to analyze and dispute such in the future.

Under 35 U.S.C. § 103, the Patent Office bears the burden of establishing a prima facie case of obviousness. In re Fine, 837 F.2d 1071, 1074 (Fed. Cir. 1988). There are four separate factual inquiries to consider in making an obviousness determination: (1) the scope and content of the prior art; (2) the level of ordinary skill in the field of the invention; (3) the differences between the claimed invention and the prior art; and (4) the existence of any objective evidence, or "secondary considerations," of non-obviousness. Graham v. John Deere Co., 383 U.S. 1, 17-18 (1966); see also KSR Int'l Co. v. Teleflex Inc., 127 S. Ct. 1727 (2007). An "expansive and flexible approach" should be applied when determining obviousness based on a combination of prior art references. KSR, 127 S. Ct. at 1739. However, a claimed invention combining multiple known elements is not rendered obvious simply because each element was known independently in the prior art. Id. at 1741. Rather, there must still be some "reason that would have prompted" a person of ordinary skill in the art to combine the elements in the specific way that he or she did. Id.; In re Icon Health & Fitness, Inc., 496 F.3d 1374, 1380 (Fed. Cir. 2007). Also, modification of a prior art reference may be obvious only if there exists a reason that would have prompted a person of ordinary skill to make the change. KSR, 127 S. Ct. at 1740-41.

Regarding claims 1, 12, and 21, the Examiner asserts that Peng in view of Kirby discloses the claimed invention. Applicant respectfully disagrees. However, in order to forward the present application toward allowance, Applicant has amended claims 1, 12, and 21 to more specifically define the claimed invention. Specifically, Applicant has amended claims 1, 12, and 21 to substantially incorporate the limitations of claims 2 and 13. As discussed in further detail below, Applicant respectfully submits that the limitations of claims 2 and 13 are not disclosed, or even suggested, by Peng and Kirby, as well as other cited references. Thus, Applicant respectfully submits that Peng and Kirby, as well as the other cited references, fail to disclose, or even suggest, a method for tracing source address of packets comprising: "querying a storage module of the first network element to identify at least one source address of a previously received packet, wherein the at least one source address of the previously received packet is recorded in a hierarchical data structure and the hierarchical data structure is based at least in part on a plurality of classes of subnet," as presently claimed.

Applicant respectfully submits that Peng fails to disclose, or even suggest, a method for tracing source addresses of packets comprising "querying a storage module of the first

network element to identify at least one source address of a previously received packet," as claimed. In contrast, Peng merely discloses a hash table used to record IP addresses that appear in a current time interval Δ_n. *See,* e.g., Page 4, Section A, Second paragraph, lines 3-5. Nowhere does Peng disclose, or even suggest, querying the hash table "to identify at least one source address of a previously received packet," as claimed. At best, Peng merely discloses comparing current counts of the hash table with an IP address database (IAD) to determine how many new IP addresses have appeared in a time slot. Additionally, if the number of packets per IP address is larger than a certain threshold, an alarm is set to indicate a bandwidth attack. *See,* e.g., Section A, Second Paragraph, lines 8-12. Thus, Peng, at best, discloses querying the hash table in order to determine current counts of new IP address of the hash table and fails to disclose, or even suggest, "querying a storage module of the first network element to identify at least one source address of a previously received packet," as claimed.

Also, the Examiner asserts, and Applicant agrees, that Peng fails to disclose, or even suggest, "routing the current packet to a second network element if at least part of a source address of the current packet matches at least part of the at least one source address of the previously received packet," as claimed.

In contrast, Peng discloses adding legitimate IP addresses to an IP Address Database (IAD), recording IP addresses that appear in a current time interval in a hash table along with a number of IP packets and a time stamp of the most recent IP packet for each IP address, and comparing the IAD to the hash table to determine the number of new IP addresses that have appeared in the current time interval. Thus, Applicant respectfully submits that Peng merely discloses recording the packet in the hash table and not "routing the current packet to a second network element," as claimed. Moreover, the source IP address monitoring (SIM) scheme of Peng merely passively monitors the packets and fails to actively rout the packets.

The Examiner asserts that Kirby remedies the deficiencies of Peng and concludes that it would have been obvious to one of ordinary skill in the art at the time the invention to modify the system of Peng to route the current packet to its destination when the source address of the packet matches an existing entry stored in the hash table in order to prevent attack traffic from being forwarded. Applicant respectfully disagrees. Specifically, Applicant respectfully submits that Peng teaches away from Kirby. As mentioned above, Peng discloses adding legitimate IP addresses to an IP Address Database (IAD), recording IP addresses that appear in a current

time interval in a hash table along with a number of IP packets and a time stamp of the most recent IP packet for each IP address, and comparing the IAD to the hash table to determine the number of new IP addresses that have appeared in the current time interval. In contrast, Kirby discloses an authorization controller 102 attached to a network port of a modified router, wherein the modified router passes to the authorization controller only packets to types (e.g., SYN, FIN) which relate to setting up, terminating, and otherwise managing a packet connection. *See*, e.g., column 3, lines 58-63. Therefore, Peng discloses calculating a number of new IP addresses that appear in a time slot, while Kirby discloses routing control of specific types of packets. Therefore, Applicant respectfully submits that it would not have been obvious to one of ordinary skill in the art at the time of the invention to utilize the routing control (e.g., specific types of packets) of Kirby in order to calculate a number of new IP addresses that appear in a time slot of Peng.

Accordingly, Applicant respectfully submits that claims 1, 12 and 21 are allowable over Peng and Kirby, as well as the other cited references.

Regarding claims 3, 4-6, 9, 14-17, 20, and 22, these claims are dependent upon independent claims 1 and 12. Thus, since

independent claims 1 and 12 should be allowable as discussed above, claims 3, 4-6, 9, 14-17, 20, and 22 should also be allowable at least by virtue of their dependency on independent claims 1 and 12. Moreover, these claims recite additional features which are not disclosed, or even suggested, by the cited references taken either alone or in combination.

In view of the foregoing, Applicant respectfully requests that the aforementioned obviousness rejection of claims 1, 3-6, 9, 12, 14-17, and 20-22 be withdrawn.

II. THE OBVIOUSNESS REJECTION OF CLAIMS 2, 13, 23, AND 24

On page 5 of the Office Action, claims 2, 13, 23, and 24 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Peng et al. ("Peng") ("Detecting Distributed Denial of Service Attacks Using Source IP Address Monitoring") in view of U.S. Patent No. 5,828,846 to Kirby et al. ("Kirby") and further in view of U.S. Patent No. 6,665,297 to Hariguchi et al. ("Hariguchi"). This rejection is hereby respectfully traversed.

Regarding claims 2 and 13, on page 5 of the Office Action, the Examiner asserts that Peng discloses that the at least one source address is recorded in a hierarchical data structure, wherein the hierarchical data structure is based at least in part on a plurality of classes of subnet. Applicant

respectfully disagrees. In contrast, Peng merely discloses a hash table used to record IP addresses that appear in a current time interval Δ_n. *See*, e.g., Page 4, Section A, Second paragraph, lines 3-5. Also, Figure 3 of Peng, merely illustrates a hash table having an IP address column, a number of packets column, and a most recent time stamp column. Thus, Applicant respectfully submits that nowhere does Peng disclose, or even suggest, that "the at least one source address of the previously received packet is recorded in a hierarchical data structure and the hierarchical data structure is based at least in part on a plurality of classes of subnet," as presently claimed.

Also, the Examiner asserts on page 6 of the Office Action, and Applicant agrees, that Peng fails to disclose, or even suggest that "the hierarchical data structure is based at least in part on a plurality of classes of subnet," as presently claimed. As discussed above, on page 5 of the Office Action, the Examiner asserts that Peng does disclose that the at least one source address is recorded in a hierarchical data structure, wherein the hierarchical data structure is based at least in part on a plurality of classes of subnet. Thus, Applicant respectfully requests that the Examiner withdraw the finality of

the Office Action and provide a clarification of the Examiner's contradictory statements in the Office Action.

In addition, on page 6 of the Office Action, the Examiner asserts that Hariguchi teaches a routing that is based on a plurality of classes of subnet and concludes that it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the system of Peng so that the hierarchical data structure is based at least in part on a plurality of classes of subnet of Hariguchi in order to improve the efficiency of searching for a specified entry in a routing table and reduce implementation cost. Applicant respectfully disagrees. In contrast, Hariguchi merely discloses a plurality of hash circuits 82, wherein each hash circuit 82 is associated with one unique prefix length. For example, the designation "hash circuit /32" indicates that the hash circuit 82-32 uses all thirty-two bits of the destination address in determining whether the destination address matches a stored destination address. The designation "hash circuit/8" indicates that the hash circuit 82-8 uses the eight leading bits of the destination address in determining whether the destination address matches a stored destination address. *See*, e.g., column 5, lines 20-31. Therefore, Applicant respectfully submits that Hariguchi merely discloses a plurality of hash circuits 82 having one unique

prefix length and fails to disclose, or even suggest, that "the at least one source address of the previously received packet is recorded in a hierarchical data structure and the hierarchical data structure is based at least in part on a plurality of classes of subnet," as presently claimed.

At this point, Applicant would like to note that claim 2 and 13 have been cancelled without prejudice, and as discussed above, the limitations of claims 2 and 13 have been substantially incorporated into claims 1, 12, and 21.

Regarding claims 23 and 24, Applicant respectfully submits that the aforementioned obviousness rejection of claims 23 and 24 has become moot in view of the deficiencies of the primary references (i.e., Peng and Kirby) as discussed above with respect to independent claim 1. That is, claims 23 and 24 are dependent upon independent claim 1 and thus inherently incorporates all of the limitations of independent claim 1. Also, the secondary reference (i.e., Hariguchi) fails to disclose, or even suggest, the deficiencies of the primary references as discussed above with respect to independent claim 1. Indeed, the Examiner does not even assert such. Thus, the combination of the secondary reference with the primary references also fails to disclose, or even suggest, the deficiencies of the primary references as discussed above with

respect to independent claim 1. Accordingly, claims 23 and 24 should be allowable over the combination of the secondary reference with the primary references at least by virtue of their dependency on independent claim 1. Moreover, claims 23 and 24 recite additional features which are not disclosed, or even suggested, by the cited references taken either alone or in combination.

In view of the foregoing, Applicant respectfully requests that the aforementioned obviousness rejection of claims 2, 13, 23, and 24 be withdrawn.

III. THE OBVIOUSNESS REJECTION OF CLAIMS 7, 8, 18, AND 19

On page 8 of the Office Action, claims 7, 8, 18, and 19 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Peng et al. ("Detecting Distributed Denial of Service Attacks Using Source IP Address Monitoring") in view of Lingafelt ("Lingafelt") (U.S. Patent Application Publication No. US2002/0147925A1). This rejection is hereby respectfully traversed.

First and foremost, Applicant respectfully submits that the aforementioned obviousness rejection of claims 7, 8, 18, and 19 is improper because the obviousness rejection of claims 7, 8, 18, and 19 fails to incorporate Kirby reference, which was the

basis for the Examiner's rejection of claims 1 and 12 from which claims 7, 8, 18, and 19 depend. Therefore, Applicant respectfully requests withdraw of the aforementioned obviousness rejection of claims 7, 8, 18, and 19.

Also, Applicant respectfully submits that the aforementioned obviousness rejection of claims 7, 8, 18, and 19 has become moot in view of the deficiencies of the primary references (i.e., Peng and Kirby) as discussed above with respect to independent claims 1 and 12. That is, claims 7, 8, 18, and 19 are dependent upon independent claims 1 and 12 and thus inherently incorporate all of the limitations of independent claims 1 and 12. Also, the secondary reference (i.e., Lingafelt) fails to disclose, or even suggest, the deficiencies of the primary references as discussed above with respect to independent claims 1 and 12. Indeed, the Examiner does not even assert such. Thus, the combination of the secondary reference with the primary references also fails to disclose, or even suggest, the deficiencies of the primary references as discussed above with respect to independent claims 1 and 12. Accordingly, claims 7, 8, 18, and 19 should be allowable over the combination of the secondary reference with the primary references at least by virtue of their dependency on independent claims 1 and 12. Moreover, claims 7, 8, 18, and 19

recite additional features which are not disclosed, or even suggested, by the cited references taken either alone or in combination.

In view of the foregoing, Applicant respectfully requests that the aforementioned obviousness rejection of claims 7, 8, 18, and 19 be withdrawn.

IV. THE OBVIOUSNESS REJECTION OF CLAIM 11

On page 9 of the Office Action, claim 11 was rejected under 35 U.S.C. § 103(a) as being unpatentable over Peng ("Detecting Distributed Denial of Service Attacks Using Source IP Address Monitoring") in view of U.S. Patent No. 5,828,846 to Kirby et al. ("Kirby") and further in view of U.S. Patent No. 5,852,630 to Langberg et al. ("Langberg"). This rejection is hereby respectfully traversed.

Applicant respectfully submits that the aforementioned obviousness rejection of claim 11 has become moot in view of the deficiencies of the primary references (i.e., Peng and Kirby) as discussed above with respect to independent claim 1. That is, claim 11 is dependent upon independent claim 1 and thus inherently incorporates all of the limitations of independent claim 1. Also, the secondary reference (i.e., Langberg) fails to disclose, or even suggest, the deficiencies of the primary

references as discussed above with respect to independent claim 1. Indeed, the Examiner does not even assert such. Thus, the combination of the secondary reference with the primary references also fails to disclose, or even suggest, the deficiencies of the primary references as discussed above with respect to independent claim 1. Accordingly, claim 11 should be allowable over the combination of the secondary reference with the primary references at least by virtue of its dependency on independent claim 1. Moreover, claim 11 recites additional features which are not disclosed, or even suggested, by the cited references taken either alone or in combination.

In view of the foregoing, Applicant respectfully requests that the aforementioned obviousness rejection of claim 11 be withdrawn.

V. CONCLUSION

In view of the foregoing, Applicant respectfully submits that the present application is in condition for allowance, and an early indication of the same is courteously solicited. The Examiner is respectfully requested to contact the undersigned by telephone at the below listed telephone number, in order to expedite resolution of any issues and to expedite passage of the

present application to issue, if any comments, questions, or suggestions arise in connection with the present application.

To the extent necessary, a petition for an extension of time under 37 CFR § 1.136 is hereby made.

Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account No. 14-1315, and please credit any excess fees to the same deposit account.

Respectfully submitted,

Hunton & Williams LLP

By: Thomas E. Anderson
Registration No. 37,063

TEA/DD

Hunton & Williams LLP
1900 K Street, N.W.
Washington, D.C. 20006-1109
Telephone: (202) 955-1500
Facsimile: (202) 778-2201

Date: March 30, 2009